



**UNITED STATES
NUCLEAR REGULATORY COMMISSION**
WASHINGTON, D.C. 20555-0001

August 6, 2019

MEMORANDUM TO: Anthony Bowers, Acting Chief
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

FROM: Shana Helton, Director **/RA/**
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

SUBJECT: NUCLEAR POWER REACTOR CYBER SECURITY PROGRAM
ASSESSMENT NEXT STEPS AND ACTION PLAN

I am writing in response to your memorandum, "Power Reactor Cyber Security Program Assessment" (July 12, 2019, Agencywide Documents Access and Management System (ADAMS) Accession Number ML19175A211). This assessment was conducted to assess the cyber security program; specifically, to seek feedback and lessons learned regarding the cyber security rule, associated guidance, licensee implementation, and the U.S. Nuclear Regulatory Commission (NRC) inspections. I commend the team for proactively seeking insights from a variety of internal and external stakeholders, to help inform any recommended program changes as we move forward.

Consistent with the discussion of next steps in the assessment, by September 20, 2019, staff should provide me with a draft action plan, for my review and approval that consolidates and prioritizes short-term and long-term improvements to the power reactor cyber security program. The action plan should identify enhancements to the cyber security program that promote regulatory efficiency and effectiveness, while continuing to provide for reasonable assurance of public health and safety and promote common defense and security. Staff should not wait for my approval of the action plan to begin efforts to adopt a risk-informed approach to the scoping of critical digital assets (CDAs) associated with emergency preparedness. The action plan should identify, as a short-term effort, recommendations regarding the appropriate scoping of CDAs that are beyond the North American Electric Reliability Corporation Critical Infrastructure Protection standards. Long-term improvements should also focus on applying a risk-informed approach to the cyber security program and should explore development of a more performance-based inspection program, including the development of performance indicators. The action plan should be developed in close coordination with regional inspection staff as well as the Federal Energy Regulatory Commission and other Federal partners. Additionally, the action plan should consider the recommendations from the Office of the Inspector General's Audit of the NRC's Cyber Security Inspections at Nuclear Power Plants (June 4, 2019, ADAMS Accession Number ML19155A317), program enhancements proposed by the Nuclear Energy Institute, and other public feedback.

CONTACT: Shana Helton, NSIR/DPCP
(301) 287 – 9104

Finally, I caution staff when initiating changes to the power reactor cyber security program. All changes should be evaluated to ensure: 1) they do not adversely impact other areas of the program; 2) guidance revisions are consistent and incorporated throughout all documents; 3) a backfit analysis is performed, if necessary; and 4) they do not constitute an unreasonable risk to public health and safety.

Please let me know if you have any questions or concerns.

NUCLEAR POWER REACTOR CYBER SECURITY PROGRAM ASSESSMENT NEXT STEPS
AND ACTION PLAN; DATED: AUGUST 6, 2019

DISTRIBUTION:

PUBLIC

ADAMS Accession No.: ML19179A032

*** (concurred via e-mail)**

OFFICE	DPCP/CSB	DPCP
NAME	B. Bergemann*	S. Helton
DATE	8/2/19	8/6/19

OFFICIAL RECORD COPY